

Raspodijeljene glavne knjige i kriptovalute

Primjene pametnih ugovora i decentralizirane financije

Stjepan Begušić, Ante Đerek, Zvonko Konstanjčar

13. siječnja 2022.



Pametni ugovori

- Javni i nepromjenjivi računalni programi pohranjeni na lancu blokova
- Sadrže podatke i funkcije
- Javno i pouzdano se izvršavaju koristeći raspodijeljeni konsenzus

Transakcije

- Mijenjaju globalno stanje - prebacuju sredstva ili pozivaju funkcije ugovora
- Iniciraju ih vanjski računi, a izvršavaju ih rudari
- U slučaju greške stanje se vraća na početno

Primjene pametnih ugovora

- **Tokeni** - kriptovalute implementirane kao pametni ugovori na Ethereum platformi
 - **Zamjenjivi tokeni** (ERC-20)
 - **Nezamjenjivi tokeni** (ERC-721)
- **Raspodijeljene autonomne organizacije (DAO)** - virtualni entitet u kojem suvlasnici kolektivno donose odluke
 - Glasačka prava predstavljena količinom tokena (*governance token*)
- Decentralizirani krediti, burze, i čitav spektar financijskih usluga - DeFi

Veza s vanjskim svijetom - izvijestitelj (*oracle*):

- Entitet koji ažurira stanje ugovora kojem su potrebne informacije (npr. trenutna cijena S&P 500 indeksa)

Sadržaj:

- Uvod i motivacija
- Stabilne kriptovalute (*stablecoin*)
- Decentralizirani *stablecoin*
- Decentralizirano kreditiranje
- Decentralizirane burze (DEX)

Živimo u svijetu centraliziranih financija:

- Centralne banke kontroliraju količinu novca
- Trgovanje se većinom vrši putem posrednika
- Kreditiranje se odvija preko banaka

Centralizirani sustav financija ima mnoge prednosti!

- Lakše upravljanje i regulacija,
- Zaštita od krađe identiteta ili gubitka osobnih informacija,
- Korisnička podrška...

Problemi centraliziranih financija

- Centralizirano upravljanje i koncentracija moći
- Ograničen pristup uslugama
- Neučinkovitost
- Nedovoljna interoperabilnost
- Netransparentnost

Primjeri:

- Transakcije kreditnim karticama koštaju do 3%
- Korisnici bez kreditnog rejtinga teško mogu doći do kredita
- Dionice službeno mijenjaju vlasnika tek 2 dana nakon trgovanja

Decentralizirane financije (*DeFi*)

Skup decentraliziranih aplikacija i organizacija koje nude financijske usluge na lancu blokova.

Volatilnost kriptovaluta je prevelika za većinu primjena.

Što ako možemo imati decentralizirani konsenzus i stabilnost cijene?

Stablecoin

Stablecoin je kriptovaluta čija je cijena vezana (eng. *pegged*) na određenu financijsku imovinu ili fiat valutu.

Centralizirani *stablecoini*:

- Izdavatelj jamči svim vlasnicima kriptovalute da za nju mogu dobiti odgovarajuću vrijednost vezane imovine
- Primjer: USD Coin (USDC), Tether (USDT) - svi korisnici mogu zamijeniti 1 USDT za 1 USD kod izdavatelja
- Potrebno vjerovati izdavatelju!

Dva tokena:

- MKR - token za upravljanje (governance) koji nosi glasačka prava za promjene u sustavu,
- DAI - stablecoin vezan (eng. *pegged*) na USD.

Glavna ideja

Vrijednost DAI tokena u odnosu na USD održava se decentralizirano, uz pomoć kolaterala i trezora (eng. *vault*) - pametnog ugovora koji prati kolateral.

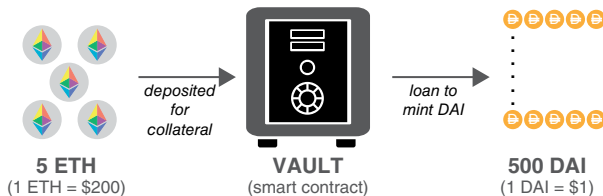
- Korisnik uplati ETH ili ERC-20 token kao kolateral u trezor
- Na temelju kolaterala korisnik može stvoriti nove DAI tokene
 - Iznos ograničen minimalnim *kolateralizacijskim omjerom*
- Korisnik u budućnosti može vratiti DAI tokene u trezor i dobiti svoj kolateral natrag

Kolateralizacijski omjer - koliko kolaterala korisnik ima u trezoru za određen iznos generiranih DAI tokena

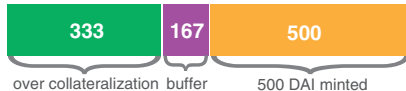
- Ako je minimalni omjer 150%, onda za 100 DAI tokena korisnik mora imati barem 150 USD u kolateralu u trezoru
- U slučaju da omjer padne ispod minimalnog (npr. 150%) - korisnik mora nadopuniti kolateral ili dolazi do likvidacije

Primjer

- *Korisnik raspolaže s 5 ETH, uz 1 ETH = 200 USD (ukupno $5 \times 200 = 1000$ USD)*
- *Neka je minimalni kolateralizacijski omjer 150%*
- *Korisnik može generirati maksimalno 667 DAI*
- *Radi sigurnosti, korisnik generira 500 DAI (omjer 200%)*



VALUE of COLLATERAL (5 ETH) = \$1,000



collateralization factor: **150%**

maximum loan: **$1,000/1.5 = 667$ DAI**

actual loan: **500 DAI**

Izvor: *DeFi and the Future of Finance*

Ako vrijednost kolaterala naraste - korisnik može generirati dodatan iznos DAI tokena.

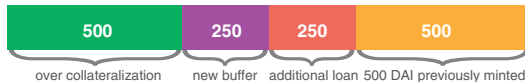
Primjer

- Ako cijena ETH naraste na 300 USD, korisnik može generirati novih 250 DAI (ako želi održati omjer od 200%).

Scenario 1

ETH appreciates 50% \$200 → \$300

VALUE of COLLATERAL (5 ETH) = \$1500



collateralization factor: 150%

maximum loan: $1,500 / 1.5 = 1,000$ DAI

actual loan: 500 DAI → (ratio now 300%)

additional loan: 250 DAI

new loan: 750 DAI → (ratio 200%)

Izvor: *DeFi and the Future of Finance*

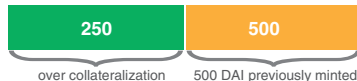
Ako vrijednost kolaterala padne do (ili ispod) minimalnog omjera:

- Korisnik može uplatiti dodatni kolateral u trezor
- Korisnik može vratiti sve DAI tokene u trezor i dobiti svoj kolateral natrag
- Drugi korisnik (*keeper*) može likvidirati ugovor
 - Proda dovoljnu količinu kolaterala za DAI tokene koje je potrebno vratiti u trezor
 - *Keeper* uzme određeni trošak za sebe
 - Ostatak kolaterala se vraća korisniku trezora

Scenario 2

ETH depreciates 25% \$200 → \$150

VALUE of COLLATERAL (5 ETH) = \$750



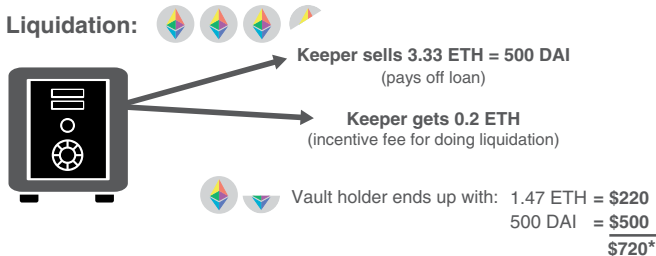
collateralization factor: 150%

maximum loan: $750/1.5 = 500$ DAI

actual loan: 500 DAI → (ratio now 150%)

Primjer

- Cijena ETH pala je na 150 USD - kolateral vrijedi 750 USD a omjer je sad 150%
- Keeper će prodati 3.33 ETH za 500 DAI i vratiti ih u trezor
- Zadržat će 0.2 ETH kao trošak, a ostatak od 1.47 ETH vraća korisniku



*Abstracts from gas fees

Dodatni mehanizmi koji potiču balans ponude i potražnje:

- Trošak za stabilnost (eng. *stability fee*)
 - Varijabilna kamata koja se naplaćuje od svih korisnika trezora koji su generirali DAI tokene
- DAI stopa štednje (eng. *DAI savings rate*)
 - Varijabilna kamata koja se isplaćuje vlasnicima DAI tokena (moraju svoje tokene uplatiti u određeni pametni ugovor da bi zaradili DSR)
 - Vrijedi da je DSR uvijek manja od troška za stabilnost
- Ograničenje duga (eng. *debt ceiling*)
 - Maksimalan broj DAI tokena koji se mogu generirati u određenom trezoru (za određenu vrstu kolaterala)

U slučaju da u likvidaciji nije moguće podmiriti dug DAI tokena, razlika se podmiruje iz naplaćenih troškova za stabilnost.

MKR token - upravljanje Maker protokolom:

- Vlasnici MKR tokena su ujedno i vlasnici protokola
- Glasuju o promjenama parametara protokola
- Mogu izglasati isplatu dividende od viška sredstava
- U slučaju da nijedan mehanizam naplate duga ne uspije, moguće je generirati nove MKR tokene i od njihove prodaje isplatiti dug
 - Time se smanjuje udio u vlasništvu svih prethodnih vlasnika MKR tokena
- U slučaju problema u radu sustava - *emergency shutdown*

Vlasnici MKR tokena

- Što uspješnije upravljaju platformom to će njihov udio u platformi više vrijediti

Keeperi

- Primaju naknade za likvidacije koje pokrenu

Korisnici - različiti scenariji:

- Trebaju sredstva a vjeruju da će vrijednost njihove imovine (ETH ili drugi tokeni) rasti i ne žele je prodati
 - Umjesto prodaje ETH za USD, mogu založiti ETH u trezor, i iskoristiti DAI (npr. DAI prodati na burzi za USD)
- Žele prodati svoj ETH ili druge tokene, ali ne žele izazvati obvezu plaćanja poreza
- Žele iskoristiti financijsku polugu za preuzimanje dodatne izloženosti ETH ili drugim tokenima
 - Npr. založe ETH, a generirani DAI koriste za kupiti još ETH

Compound protokol - glavna ideja

- Korisnici mogu zaključati svoja sredstva u Compound protokol kao kolateral
- Korisnici mogu uzeti kredit u bilo kojim sredstvima drukčijima od svog kolaterala
- Iznos duga ograničen je kolateralizacijskim omjerom

Compound generalizira principe Maker protokola na više tokena u Ethereum sustavu (nije ograničen samo na DAI):

- Implementira decentralizirano kreditiranje u više valuta
- Sav dug (posuđeni tokeni ili ETH) dolazi od likvidnosti koju su neki (drugi) korisnici uplatili
- Svi dužnici plaćaju jednaku varijabilnu kamatnu stopu, svi pružatelji likvidnosti primaju jednaku varijabilnu kamatnu stopu

Kolateralizacijski omjer u Compound protokolu:

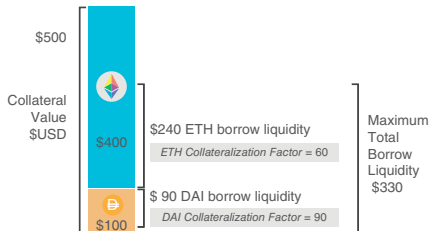
- Svaki token kojeg platforma podržava ima vlastiti *faktor kolateralala* - od 0% do 90%
 - Volatilnije valute imaju niži faktor kolateralala
- Ukupni faktor kolateralala nekog korisnika:

$$\sum_i \text{Udio kolateralala u valuti } i \cdot \text{Faktor kolateralala valute } i$$

- Odgovarajući kolateralizacijski omjer je $1/\text{faktor kolateralala}$

Primjer

- *Korisnik je uplatio 100 DAI tokena vrijednosti 100 USD i 2 ETH ukupne vrijednosti 400 USD (ukupno 500 USD)*
 - *Udio DAI u kolateralu je 20%, a ETH 80%*
- *Neka je faktor kolaterala za DAI 90% a za ETH 60%*
- *Ukupni faktor kolaterala korisnika je:*
 $0.2 \cdot 90\% + 0.8 \cdot 60\% = 66\%$ *(kolateralizacijski omjer 151%)*
- *Korisnik može posuditi 330 USD protuvrijednosti*



Collateralization Ratio

$$= \frac{\$500 \text{ collateral}}{\$330 \text{ borrow liquidity}} = 151\%$$

Also calculated as
 $100 / (0.8 \times 60 + 0.2 \times 90)$

Kamatne stope u Compoundu

- Obračunavaju se svaki blok
- Određuje ih ukupna iskorištenost u protokolu (*utilization*) - omjer posuđenih i zaključenih sredstava

Kamatna stopa za dužnike:

- Osnovna formula: $r_b = \text{base rate} + \text{slope} \cdot \text{utilization}$

Kamatna stopa za pružatelje likvidnosti (LP):

- $r_{lp} = (r_b \cdot \text{utilization})(1 - \text{reserve factor})$

Primjer

- *Neka je zaključano 100 mil. DAI, a posuđeno 50 mil. DAI*
 - *Iskorištenost je 50%*
- *Parametri: base rate = 1%, slope = 10%, reserve factor = 0%*
- *Kamatna stopa za dužnike: $1\% + 0.5 \cdot 10\% = 6\%$*
- *Kamatna stopa za pružatelje likvidnosti: $0.5 \cdot 6\% = 3\%$*

Kamata od 6% na posuđenih 50 mil. DAI (ukupno 3 mil. DAI) raspoređena je na svih zaključanih 100 mil. DAI (što odgovara 3%).

- U praksi se kamata računa na razini bloka, a izražava u godišnjoj razini (APY).

Kako je implementirana uplata i posuđivanje? Kako se kamate naplaćuju i isplaćuju?

cToken

- ERC-20 token koji predstavlja centralni ugovor za sve uplate i posuđivanja za određenu valutu
- cETH, cDai, CUSDT...

Uplaćivanje sredstava:

- Korisnik uplati sredstva (npr. DAI) na odgovarajući cToken ugovor
- Po trenutnom cjeniku generira cTokene (cDAI) koji su pridruženi njegovoj adresi (1 DAI nije uvijek 1 cDAI)
- U bilo kojem trenutku korisnik može vratiti svoje cTokene u ugovor i dobiti originalna sredstva + kamatu

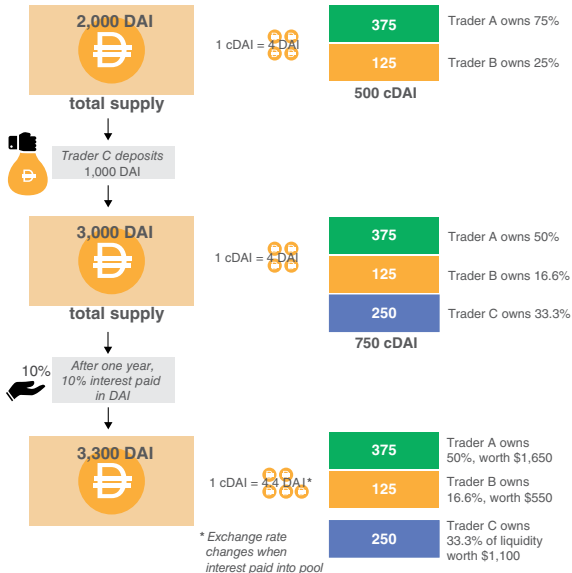
Posuđivanje sredstava i vraćanje duga:

- Korisnik koji je uplatio kolateral može zatražiti sredstva od cToken ugovora valute koju želi posuditi
- Maksimalni iznos je određen sredstvima koje je uplatio u protokol i faktorom kolaterala
- Iznos koji je potrebno vratiti da bi zatvorio dug povećava se s vremenom, ovisno o kamatnoj stopi r_b
- U bilo kojem trenutku korisnik može vratiti posuđena sredstva i zatvoriti dug

Cjenik (token - cToken):

- Cijena je direktno određena količinom valute u cToken ugovoru i izdanih cTokena

Compound



Upravljanje Compound protokolom:

- Parametri: faktor kolateralala za svaku valutu, parametri kamatnih stopa...
- COMP token - slično kao u Maker protokolu, vlasnici tokena glasuju o promjenama protokola

Protokol za kreditiranje sličan Compoundu, uz neke inovacije:

- Mogućnost otvaranja novih tržišta koja nisu povezana s ostalima - imaju vlastite bazene likvidnosti
- P2P zajmovi drugim stranama (*credit delegation*)
- Nekolateralizirani (trenutni) zajmovi - *flash loans*

Flash loan

Trenutni zajam (*flash loan*) je nekolateralizirani zajam koji se vraća unutar iste transakcije.

- Korisnik u određenoj transakciji može posuditi sredstva, koristiti se njima u istoj transakciji i na kraju ih vratiti natrag.
- U slučaju da dužnik ne može vratiti zajam, transakcija se neće izvršiti ispravno.
- Kolateral nije nužan.

Primjer

- *Korisnik je uplatio 100 ETH (svaki po cijeni 200 DAI) u Compound protokol*
- *Uzeo je zajam na 10.000 DAI i s njima kupio još 50 ETH, koje je također uplatio u Compound*
- *Neka je kamatna stopa za DAI dužnike u Compoundu 15% a u Aave protokolu 5%*
- *Kako refinancirati ovaj dug što efikasnije?*
- *Moguće je sve ove transakcije jednu po jednu "odmotati":*
 - *Isplatiti ETH iz zadnjeg ugovora natrag i prodati ih za DAI,*
 - *Vratiti DAI u prvi ugovor i dobiti originalne ETH natrag,*
 - *Uplatiti ETH u Aave, uzeti zajam u DAI, kupiti ETH, uplatiti opet u Aave.*
 - *Neefikasno!*

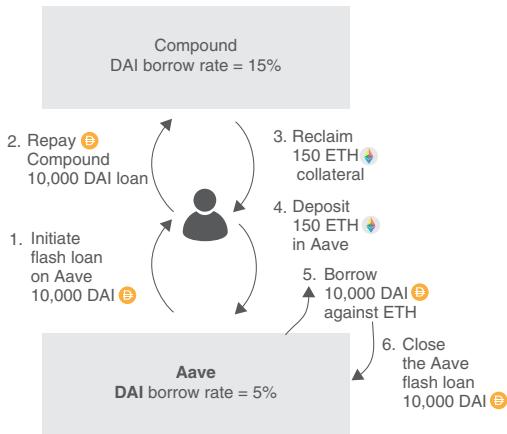
Primjer

Alternativa - preko trenutnog zajma:



- *Korisnik uzme trenutni zajam na 10.000 DAI na Aave platformi,*
- *U istoj transakciji isplati ETH iz zadnjeg ugovora i vrati dug u prvom ugovoru - dobije svih 150 ETH natrag,*
- *Uplati 150 ETH u Aave i koristeći ih kao kolateral zaduži se za 10.000 DAI (po stopi od 5%),*
- *Tih 10.000 DAI koristi za vratiti zajam na kraju transakcije.*

Before

+ 150 ETH (collateral) 
- 10,000 DAI (loan)  at 15% interest



After

+ 150 ETH (collateral) 
- 10,000 DAI (loan)  at 5% interest

Ilvzor: *DeFi and the Future of Finance*

Decentralizirane burze kriptovaluta (DEX)

Glavni zadatak decentraliziranih burzi je razmjena kriptovaluta između korisnika bez posrednika ili skrbništva.

Dva mehanizma:

- Povezivanje preko knjige naloga (*order book matching*)
 - Implementacija knjige naloga u pametnom ugovoru
 - Slanje svakog naloga zahtijeva transakciju na lancu blokova
- Automatizirani održavatelji tržišta (*automated market maker, AMM*)
 - Pametni ugovor koji drži sredstva u obje valute u određenom valutnom paru
 - Korisnici mogu kupiti jednu valutu za drugu direktno od AMM-a

Kako AMM određuje cijenu po kojoj nudi valute?

Primjer

Što ako postavi fiksnu cijenu (npr. $1 \text{ ETH} = 200 \text{ DAI}$)?

- Ako se tržišna cijena promijeni, korisnici mogu kupiti skuplju valutu s AMM-a i potpuno isprazniti njene količine s ugovora*
- Funkcija cijene mora biti takva da je skuplje kupovati onu valutu koje ima manje na ugovoru

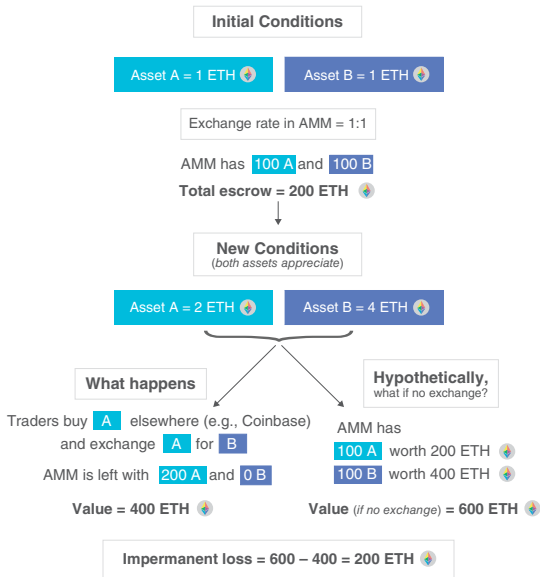
Prednosti AMM-ova:

- Uvijek dostupni
- Bilo koji ugovor može koristiti likvidnost AMM-a

Rizici/mane:

- Nestalni gubitak (*impermanent loss*)

Decentralizirane burze



Uniswap protokol

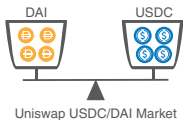
- Funkcija cijene je takva da je umnožak stanja valuta konstantan
- Likvidnost se prikuplja iz bazena sredstava koje korisnici ulažu
- Svako trgovanje ima određeni trošak (0.3%) koji se isplaćuje pružateljima likvidnosti kao zarada
- Tržište za svaki valutni par implementirano kroz pametni ugovor (slično cToken mehanizmu u Compoundu)
- Decentralizirano upravljanje preko UNI tokena

Funkcija cijene:

- Ako su količine valuta x i y , onda umnožak $k = x \cdot y$ mora biti konstantan
- Cijena je određena omjerom x/y

Primjer

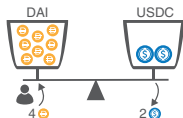
- *Neka je na AMM ugovoru 4 USDC i 4 DAI*
 - $k = 4 \cdot 4 = 16$
 - *Trenutni omjer (cijena): 1 USDC = 1 DAI*
- *Korisnik želi kupiti USDC, ima 4 DAI:*
 - *Da bi ostalo $k = 16$, korisnik može dobiti 2 USDC*
 - *Cijena po kojoj je kupio je 1 USDC = 2 DAI*
- Promjenu u cijeni zbog ograničene likvidnosti nazivamo proklizavanje (*slippage*).
- Koliko bi cijena kliznula da je na AMM-u bilo 100 USDC i 100 DAI?



Instantaneous
exchange rate = 1 🟡 = 1 🔵
Invariant (K) = 4 🟡 x 4 🔵 = 16

Scenario A

Exchange 4 DAI



Invariant = $K = 8 \text{ 🟡} \times 2 \text{ 🔵} = 16$
Hence, 4 DAI exchanged for 2 USDC

Scenario B

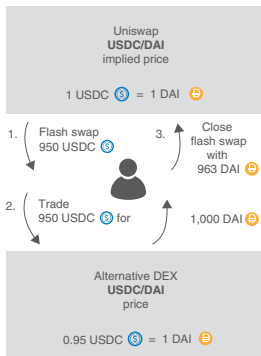
Exchange 4 DAI
but contract has more liquidity, 100 DAI, 100 USDC



Instantaneous
exchange rate = 1 🟡 = 1 🔵
Before $K = 100 \times 100 = 10,000$
After $K = 104 \times 96.15 = 10,000$
Implied price = 1.04 🟡 = 1 🔵

Slično Aave protokolu, Uniswap nudi tzv. *flash swap*:

- Sredstva je moguće dobiti prije nego se uplati druga valuta, ukoliko se transakcija uspješno završava uplatom druge valute



4. Slippage = 10 DAI, so 960 DAI
Fee = $.003 \times 960 = 3$ DAI
Swap done at $960 + 3 = 963$ DAI
Profit = $1,000 - 963 = 37$ DAI

Izvor: *DeFi and the Future of Finance*

Druge primjene:

- Tokenizacija - kako imovinu koja nije na lancu blokova (BTC, USD, zlato...) predstaviti tokenima
- Financijske izvedenice - opcije, futures ugovori i druga sintetička financijska imovina
- Osiguranje i druge financijske usluge na lancu blokova

Glavni rizik centraliziranih financija koji je eliminiran u DeFi - rizik druge strane:

- Npr. rizik da će burza ili dužnik bankrotirati

Rizici:

- Rizik pametnih ugovora - napadi zbog sigurnosih propusta u dizajnu ugovora (primjer: TheDAO)
- Rizik upravljanja - protokoli kojima se upravlja decentralizirano se mogu napasti kupovinom *governance* tokena (primjer: TSD)
- Rizik *oraclea* - izvori informacija mogu biti napadnuti ili kompromitirani
- Regulatorni rizik - regulatorne agencije mogu zabraniti određene protokole ili otežati njihov rad
- Ostali rizici: rizik skrbništva, utjecaj na okoliš, skaliranje...

Harvey, Ramachandran, Santoro, *DeFi and the Future of Finance*, Wiley, 2021.

- I. Introduction - Five Key Problems of Centralized Financial Systems, Implications (str. 1 - 7)
- III. DeFi Infrastructure - Oracles, Stablecoins, Decentralized Applications (str. 23 - 28)
- IV. DeFi Primitives - Transactions, Fungible Tokens, Non-fungible Tokens (str. 29 - 38)
- IV. DeFi Primitives - Swap, Collateralized Loans, Flash (Uncollateralized) Loans (str. 50 - 57)
- VI. DeFi Deep Dive - Credit/Lending, Decentralized Exchange (str. 69 - 105)